PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-271104
(43)Date of publication of application : 09.10.1998

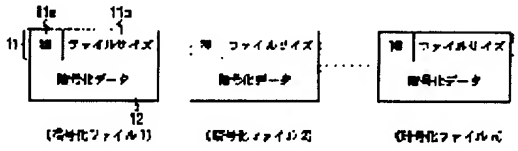
(51)Int.Cl. H04L 9/08
G06F 12/00
G06F 12/14

(21)Application number : 09-069944
(22)Date of filing : 24.03.1997

(71)Applicant : HITACHI INF SYST LTD
(72)Inventor : ITO MASARU

(54) CIPHERING METHOD AND DECIPHERINC METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To safely and surely maintain security by using a file cipher key obtained based on the N kinds, master keys and intrinsic attribute information respectively corresponding to the N files, storing ciphered files for which the respective files are ciphered along with the respective kinds and the attribute information and then, eliminating the file cipher keys and the master key used for ciphering.
SOLUTION: For one master key (m) generated first, the (n) kinds corresponding to the (n) files to be ciphered are obtained corresponding to a prescribed kind division rule. Thereafter, based on the intrinsic attribute information and the master key for the respective files, the obtained file cipher key is used and the (n) files are respectively ciphered. Then, the (n) kinds 11a are stored along with a file size 11b which is the attribute information in the respective header parts 11 of the respective corresponding ciphered files 1-(n). Thereafter, the (n) file cipher keys and the master key are eliminated. Thus, the management burdens of the ciphered files and the cipher key are reduced.



LEGAL STATUS

[Date of request for examination] 21.09.1999
[Date of sending the examiner's decision of rejection] 09.09.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－271104

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｚ
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ｈ
	12/14	３２０		12/14	３２０Ｂ

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願平9－69944

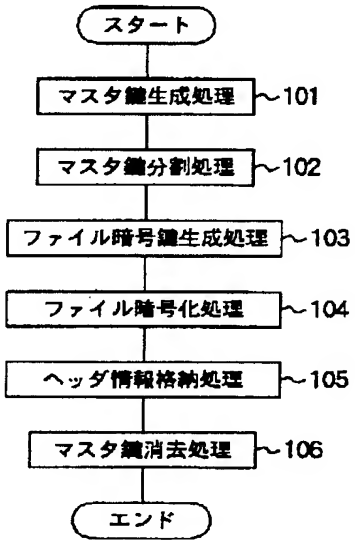
(22)出願日　平成９年(1997)３月24日

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　伊藤　優
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　弁理士　武　顕次郎

(54)【発明の名称】　暗号化方法及び復号化方法

(57)【要約】
【課題】　暗号化方法及び復号化方法に関し、少ない管理負担で従来より安全かつ確実に機密保持を図る。
【解決手段】　暗号化では、最初に、乱数発生装置で生成したマスタ鍵を分割して、Ｎ個のファイルに対応するＮ個の種を求める。そして、Ｎ個のファイルごとに、ファイルの属性情報及びマスタ鍵に基づいてファイル暗号鍵を求め、このファイル暗号鍵を用いて、ファイルを暗号化して暗号化ファイルを生成し、種及び属性情報を暗号化ファイル中に格納する。最後に、マスタ鍵を消去する。復号化では、最初に、暗号化ファイル中に格納された種を取り出し、この取り出した複数の種からマスタ鍵を復元する。そして、Ｎ個の暗号化ファイルごとに、暗号化ファイル中に格納された属性情報及びマスタ鍵に基づいてファイル暗号鍵を求め、このファイル暗号鍵を用いて、暗号化ファイルを復号化して元のファイルを復元する。

【図　１】



【特許請求の範囲】
【請求項１】　Ｎ個のファイルに共通なマスタ鍵を用いてＮ個のファイルのそれぞれを暗号化したＮ個の暗号化ファイルを生成する暗号化方法において、最初にひとつのマスタ鍵を生成し、
前記マスタ鍵を所定の種分割規則にしたがって分割して前記Ｎ個のファイルのそれぞれに対応するＮ個の種を求め、
前記Ｎ個のファイルの各々に固有の属性情報と前記マスタ鍵とに基づいて、当該ファイルに対応する前記ファイル暗号鍵を求め、
このファイル暗号鍵を用いて当該ファイルを暗号化して、当該ファイルに対応する前記暗号化ファイルを生成し、
前記種及び前記属性情報を前記暗号化ファイルとともに格納した後、
暗号化に用いたすべての前記ファイル暗号鍵及び前記マスタ鍵を消去することを特徴とする暗号化方法。
【請求項２】　前記種分割規則にしたがって求めた前記Ｎ個の種のうち、前記Ｎ個を超えない所定のｋ個の前記種に基づいて前記マスタ鍵を生成し得ることを特徴とする請求項１に記載の暗号化方法。
【請求項３】　Ｎ個のファイルに共通なマスタ鍵を用いてＮ個の暗号化ファイルのそれぞれを復号化したＮ個のファイルを復元する復号化方法において、
複数の前記暗号化ファイルとともにそれぞれ格納された所定の種を取り出し、
所定の種復元規則にしたがって、取り出した複数の前記種から前記マスタ鍵を復元し、
前記Ｎ個の暗号化ファイルの各々とともに格納された固有の属性情報と前記マスタ鍵とに基づいて、前記Ｎ個の暗号化ファイルに対応する前記Ｎ個のファイル暗号鍵を求め、
前記Ｎ個のファイル暗号鍵を用いて前記Ｎ個の暗号化ファイルを復号化して、前記Ｎ個のファイルを復元することを特徴とする復号化方法。
【請求項４】　前記マスタ鍵を生成するために、少なくとも、前記Ｎ個を超えない所定のｋ個の前記種を必要とすることを特徴とする請求項３記載の復号化方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は暗号化方法及び復号化方法に係り、特に、安全かつ確実に機密保持が図れる暗号化方法及び復号化方法に関する。
【０００２】
【従来の技術】近年、パソコンやワークステーションを用いて文書や図面の作成・保管を行うことが一般的になりつつある。そして、こうした文書や図面の中には、その記述内容が部外者に知られたときの影響が大きく、機密保持の対策を施す必要のあるものが少なくない。
【０００３】上述した機密保持の対策の代表的なものとして、暗号化技術が知られている。暗号化技術で機密保持の対策を図る場合は、機密保持の対象である文書や図面が格納されたファイルを所定の暗号化アルゴリズムにしたがって暗号化し、そのままでは判読不能な暗号化ファイル及びこの暗号化ファイルから元のファイルを復元するとき利用する暗号鍵を生成する。そして、誰でも内容を判読可能な暗号化前のファイルを破棄するとともに、生成した暗号化ファイル及び暗号鍵をそれぞれ別個に保管し、特に暗号鍵については、文書や図面の作成に関わる関係者のみが利用できるよう管理する。
【０００４】このような暗号化技術による機密保持では、上述した暗号鍵が部外者に知られた場合、その部外者は、この暗号鍵を利用して暗号化ファイルから元のファイルを復元し、機密保持の対象である文書や図面の内容を判読できるので、機密保持の対策が無効になってしまう。また、保管中の暗号鍵の管理を誤って紛失した場合、関係者でさえも暗号化ファイルから元のファイルを復元不能となり、事実上、機密保持の対象である文書や図面を紛失して再利用できなくなってしまう。そこで、暗号化技術による機密保持に際しては、部外者に知られないよう確実に暗号鍵を保管しなければならない。
【０００５】上述した点を考慮した暗号鍵の保管方法のひとつとして、同一の暗号鍵をＩＣカード及びＦＤ（フロッピーディスク）などの可搬媒体に格納し、これらのＩＣカード及びＦＤをそれぞれ保管する方法が知られている。そして、ＩＣカードの場合、暗号鍵とともに、この暗号鍵の利用者が正当な関係者か否か認証するためのソフトウェアを搭載することが一般的に行われている。したがって、暗号鍵を格納したＩＣカードが部外者の手に渡ったとしても、そのＩＣカードに搭載されたソフトウェアによる認証で正当な関係者として認められるための利用者コードなどをその部外者が知らなければ、ＩＣカードに格納された暗号鍵が部外者に知られることはない。
【０００６】一方、特開平７－５６５０７号公報に記載された暗号化技術では、機密保持の対象である文書や図面を含むファイルを暗号化して生成した暗号化ファイルと、ファイルを復元するための暗号鍵である鍵データを公開鍵暗号アルゴリズムで暗号化した暗号化鍵データとを一緒に保管する。ここで、鍵データを公開鍵暗号アルゴリズムで暗号化する際には、常に同一の公開鍵を用いることとし、この公開鍵に対応する秘密鍵は別個に厳重に保管・管理しておく。
【０００７】この暗号化技術の場合、通常は、暗号化ファイルと別個に保管してある暗号鍵を用いて元のファイルを復元する。また、万一暗号鍵を紛失したときは、上述した公開鍵に対応する秘密鍵を用いて、暗号化ファイルとともに保管してある暗号化鍵データから暗号鍵を復元した後、この暗号鍵を用いて元のファイルを復元す

る。

【０００８】

【発明が解決しようとする課題】上述した可搬媒体を用いた暗号鍵の保管方法では、暗号鍵を保管している可搬媒体の紛失が暗号鍵の紛失と等しく、可搬媒体の管理を誤ると機密保持の対象である文書や図面の内容が失われてしまうという問題点があった。

【０００９】また、各々の暗号化ファイルに対応する多数の暗号鍵を保管する必要が生じることから多数の可搬媒体の保管・管理を行わなければならず、管理負担が重くなってしまうという問題点があった。

【００１０】さらに、上述したＩＣカードなどの可搬媒体に搭載されたソフトウェアによる認証で正当な関係者として認められるための利用者コードなどを部外者に知られてしまった場合、暗号鍵及びその暗号鍵で復元される元のファイルの内容を部外者に知られる危険性があるので、必ずしも確実に機密保持が図れるとは限らないという問題点があった。

【００１１】また、上述した特開平７－５６５０７号公報記載の暗号化技術でも、元のファイルを復元するための暗号鍵を部外者に知られてしまった場合、その暗号鍵及びその暗号鍵で復元されるファイルの内容を部外者に知られる危険性があるので、可搬媒体を用いた暗号化技術と同様、必ずしも確実に機密保持が図れるとは限らないという問題点があった。

【００１２】したがって本発明の目的は、上記の問題点を解決して、少ない管理負担で従来より安全かつ確実に機密保持が図れる暗号化方法及び復号化方法を提供することにある。

【００１３】

【課題を解決するための手段】上記の目的を達成するため、本発明の請求項１に係る暗号化方法は、Ｎ個のファイルに共通なマスタ鍵を用いてＮ個のファイルのそれぞれを暗号化したＮ個の暗号化ファイルを生成する暗号化方法において、最初にひとつのマスタ鍵を生成し、前記マスタ鍵を所定の種分割規則にしたがって分割して前記Ｎ個のファイルのそれぞれに対応するＮ個の種を求め、前記Ｎ個のファイルの各々に固有の属性情報と前記マスタ鍵とに基づいて、当該ファイルに対応する前記ファイル暗号鍵を求め、このファイル暗号鍵を用いて当該ファイルを暗号化して、当該ファイルに対応する前記暗号化ファイルを生成し、前記種及び前記属性情報を前記暗号化ファイルとともに格納した後、暗号化に用いたすべての前記ファイル暗号鍵及び前記マスタ鍵を消去ものである。

【００１４】また、本発明の請求項２に係る暗号化方法は、上記請求項１に係る発明において、前記種分割規則にしたがって求めた前記Ｎ個の種のうち、前記Ｎ個を超えない所定のｋ個の前記種に基づいて前記マスタ鍵を生成し得るものである。

【００１５】また、本発明の請求項３に係る復号化方法は、Ｎ個のファイルに共通なマスタ鍵を用いてＮ個の暗号化ファイルのそれぞれを復号化したＮ個のファイルを復元する復号化方法において、複数の前記暗号化ファイルとともにそれぞれ格納された所定の種を取り出し、所定の種復元規則にしたがって、取り出した複数の前記種から前記マスタ鍵を復元し、前記Ｎ個の暗号化ファイルの各々とともに格納された固有の属性情報と前記マスタ鍵とに基づいて、前記Ｎ個の暗号化ファイルに対応する前記Ｎ個のファイル暗号鍵を求め、前記Ｎ個のファイル暗号鍵を用いて前記Ｎ個の暗号化ファイルを復号化して、前記Ｎ個のファイルを復元するものである。

【００１６】また、本発明の請求項４に係る復号化方法は、上記請求項３に係る発明において、前記マスタ鍵を生成するために、少なくとも、前記Ｎ個を超えない所定のｋ個の前記種を必要とするものである。

【００１７】

【発明の実施の形態】以下、本発明の暗号化方法及び復号化方法の実施の形態を図面を用いて詳細に説明する。

【００１８】図１は、本発明の暗号化方法の一実施形態によるファイルの暗号化処理の流れを示すフローチャートである。同図中、最初のステップ１０１のマスタ鍵生成処理では、例えばコンピュータシステムのメモリ内で、利用者が任意に入力したフレーズ情報や時刻情報などを種として乱数を発生する乱数発生装置を用いて、後述する複数のファイル暗号鍵の元になるマスタ鍵ｍ（ｍはマスタ鍵を表すビット列）を生成する。続くステップ１０２のマスタ鍵分割処理では、所定の種分割規則である「Secret Shairingの多項式」にしたがってマスタ鍵ｍを分割し、暗号化しようとするｎ個のファイルに対応するｎ個の種を求める。ここで、「SecretShairingの多項式」は、次の数式（１）で表される。

$$f(x)=(m+A_1x+A_2x^2+A_3x^3+\cdots\cdots+A_{k-1}x^{k-1}) \mod r$$

ただし、ｒは任意の素数（ｍ＜ｒ）を、

“ｓ mod ｔ”はｓをｔで割った剰余を、

ｋはしきい値を、それぞれ表す。

……（１）

そして、ｎ個の種は、この数式（１）に整数値ｉ（ｉ＝１，２，……ｎ）をそれぞれ代入することにより求められる。

【００１９】上述したマスタ鍵分割処理でｎ個の種を求めた後、ステップ１０３のファイル暗号鍵生成処理では、暗号化しようとするファイルごとに、そのファイルに固有の属性情報、例えばファイルサイズＮｉと、上記マスタ鍵ｍとに基づいて、そのファイルの暗号化に用いるファイル暗号鍵Ｋｉを求める。すなわち、ファイル暗号鍵Ｋｉは、次の数式（２）で求められる。

Ｋｉ＝ｇ（ｍ，Ｎｉ）

ただし、ｇ（ｘ）は一方向性関数を表す。

……（２）

具体的な一方向性関数としては、例えばＲＳＡ暗号の暗号化変換関数を利用した場合、ファイル暗号鍵Ｋｉは、次の数式（３）で求められる。

Ｋｉ＝(Ｎｉ)^{e} mod m……（３）。

【００２０】このように、ファイル暗号鍵生成処理でファイルごとにファイル暗号鍵を求めた後、ステップ１０４のファイル暗号化処理では、求めたｎ個の異なるファイル暗号鍵を用いてｎ個のファイルをそれぞれ暗号化する。そして、ステップ１０５のヘッダ情報格納処理では、先にステップ１０２のマスタ鍵分割処理で求めたｎ個の種を、それぞれ対応する暗号化ファイルのヘッダ部に、属性情報であるファイルサイズとともに格納する。最後に、ステップ１０６のマスタ鍵消去処理では、ｎ個のファイル暗号鍵の元になったマスタ鍵ｍを消去する。

【００２１】図２は、図１の暗号化処理で生成される暗号化ファイルの基本構成を示す図である。同図に示すように、それぞれの暗号化ファイルは、ヘッダ部１１とデータ部１２からなっている。そして、ヘッダ部１１には、マスタ鍵から分割された種１１ａ及び対応するファイルサイズ１１ｂが上述したヘッダ情報格納処理によって格納される。これらｎ個の暗号化ファイルは、それぞれ異なる記憶装置や可搬媒体に分散して保管する。

【００２２】図３は、本発明の復号化方法の一実施形態によるファイルの復号化処理の流れを示すフローチャートである。同図中、最初のステップ２０１のヘッダ情報抽出処理では、図２に示した暗号化ファイルのひとつを参照し、そのヘッダ情報から上述した種を抽出する。続くステップ２０２では、これまでに抽出した種の個数がしきい値ｋを超えたか否かを判定し、抽出した種の個数がしきい値ｋを超えるまで、各暗号化ファイルのヘッダ部から種及びファイルサイズを抽出する。そして、抽出した種の個数がしきい値ｋを超えた場合（ステップ２０２＝Ｙｅｓ）、ステップ２０３のマスタ鍵復元処理で、前述した「Secret　Shairingの多項式」に対応する種復元規則にしたがって、これらｋ個以上の種からマスタ鍵ｍを復元し、続くステップ２０４のファイル暗号鍵生成処理では、図１中のステップ１０３に示した処理と同様、復号化しようとする暗号化ファイルごとに、その暗号化ファイルのヘッダ部に格納されたファイルサイズと上述のステップ２０３で復元したマスタ鍵ｍとに基づいて、その暗号化ファイルの復号化に用いるファイル暗号鍵を求める。最後に、ステップ２０５のファイル復号化処理では、ステップ２０４で求めた各々のファイル暗号鍵を用いて対応する暗号化ファイルの復号化を行い、元のファイルを復元する。

【００２３】上述した本実施形態の暗号化方法及び復号化方法によれば、まとめて暗号化したＮ個の暗号化ファイルを復号化するためのファイル暗号鍵は、Ｎ個の暗号化ファイルのヘッダ部に格納された種に基づいて復元されるマスタ鍵から生成可能であり、暗号化ファイルと別個にファイル暗号鍵を保管しておく必要がない。このため、従来のように暗号鍵を紛失して暗号化ファイルに格納した機密保持の対象である文書や図面の内容が失われてしまう懸念がなくなる。また、部外者はファイル暗号鍵を直接入手できないので、確実に機密保持が図れる。また、暗号化ファイルと暗号鍵とを別個に管理する必要がないので、管理負担の軽減を図ることができる。さらに、Ｎ個の暗号化ファイルのうちのいくつかが利用できなくなっても、しきい値ｋを上回る個数の暗号化ファイルがあればマスタ鍵を復元でき、残りの暗号化ファイルを復号化できる。

【００２４】

【発明の効果】以上詳しく説明したように、本発明の暗号化方法及び復号化方法によれば、まとめて暗号化したＮ個の暗号化ファイルを復号化するためのファイル暗号鍵は、Ｎ個の暗号化ファイルのヘッダ部に格納された種に基づいて復元されるマスタ鍵から生成可能であり、暗号化ファイルと別個にファイル暗号鍵を保管しておく必要がない。このため、従来のように暗号鍵を紛失して暗号化ファイルに格納した機密保持の対象である文書や図面の内容が失われてしまう懸念がなくなる。また、部外者はファイル暗号鍵を直接入手できないので、確実に機密保持が図れる。また、暗号化ファイルと暗号鍵とを別個に管理する必要がないので、管理負担の軽減を図ることができる。さらに、Ｎ個の暗号化ファイルのうちのいくつかが利用できなくなっても、しきい値ｋを上回る個数の暗号化ファイルがあればマスタ鍵を復元でき、残りの暗号化ファイルを復号化できる。したがって、少ない管理負担で従来より安全かつ確実に機密保持を図ることができる。

【図面の簡単な説明】

【図１】本発明の暗号化方法の一実施形態によるファイルの暗号化処理の流れを示すフローチャートである。

【図２】図１の暗号化処理で生成される暗号化ファイルの基本構成を示す図である。

【図３】本発明の復号化方法の一実施形態によるファイルの復号化処理の流れを示すフローチャートである。

【符号の説明】

ｍ　マスタ鍵

ｋ　しきい値

１１　ヘッダ部

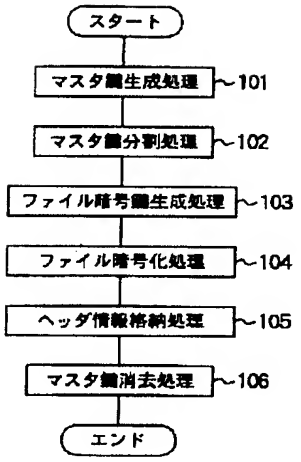
１１ａ　マスタ鍵を分割して得られた種

１１ｂ　ファイルサイズ

１２　データ部

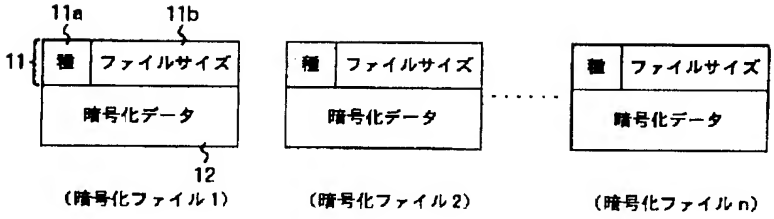
【図１】

【図 1】



【図２】

【図 2】



【図３】

【図 3】